Kekuatan Intelijen Singapura: Struktur, Aliansi, dan Teknologi 10 Tahun Terakhir

Description

Pendahuluan

Sebagai negara kota dengan lingkungan geo-politik kompleks, Singapura sangat menekankan kemampuan intelijennya untuk menjamin keamanan nasional. Dalam sepuluh tahun terakhir, arsitektur intelijen Singapura mengalami transformasi signifikan, mulai dari restrukturisasi organisasional hingga modernisasi teknologi, guna menghadapi spektrum ancaman baru seperti terorisme transnasional, spionase siber, dan perang informasi. Laporan analitis ini membahas tujuh aspek kunci: struktur organisasi intelijen Singapura, ekosistem pengetahuan think tank, aliansi strategis internasional, inovasi teknologi intelijen, strategi SDM dan rekrutmen, aktivitas regional (khususnya di Asia Tenggara), serta evaluasi risiko dan kelemahan model intelijen Singapura.

Struktur dan Organisasi Intelijen Singapura

Singapura memiliki tiga lembaga intelijen utama dengan fungsi berbeda, yaitu Internal Security Department (ISD) untuk keamanan domestik, Security and Intelligence Division (SID) untuk intelijen luar negeri, dan Military Intelligence dalam Angkatan Bersenjata Singapura yang kini berwujud Digital and Intelligence Service (DIS). Ketiga lembaga ini beroperasi dalam kerangka koordinasi nasional yang terpusat:

- Internal Security Department (ISD): Didirikan pada masa kolonial sebagai Special Branch dan direorganisasi pasca-kemerdekaan, ISD berada di bawah Kementerian Dalam Negeri (Ministry of Home Affairs). ISD menangani ancaman internal seperti terorisme domestik, spionase, subversi politik, dan isu keamanan dalam negeri lainnya[1]. Dengan kewenangan berdasarkan Internal Security Act, ISD dapat melakukan deteksi dini dan tindakan pencegahan (misalnya penangkapan tersangka teroris Jemaah Islamiyah pada 2001-2002). ISD memiliki sejarah panjang sejak era ancaman komunis, dan bertransformasi untuk menghadapi radikalisasi individu “self-radicalised” di era modern[2].

- Security and Intelligence Division (SID): SID adalah agensi intelijen eksternal Singapura yang bernaung di bawah Kementerian Pertahanan (MINDEF), namun melapor langsung ke Kantor Perdana Menteri[3][4]. Didirikan tahun 1966 tak lama setelah kemerdekaan, SID bertugas mengumpulkan dan menganalisis informasi dari seluruh dunia yang berdampak pada keamanan nasional dan kepentingan Singapura[5]. Walau secara administratif di MINDEF, SID otonom dan sangat rahasia; personelnya dikenal hanya oleh pejabat puncak pemerintah[4]. Direktur SID berpangkat setara Permanent Secretary dan sejak 1970-an melapor langsung ke PMO (sebelumnya melapor ke Menteri Pertahanan)[4]. Fokus SID mencakup isu geopolitik, hubungan luar negeri, terorisme transnasional dan ancaman siber[1]. SID bekerja dengan metode HUMINT (pengumpulan informasi manusia), SIGINT (intersepsi sinyal), analisis strategis, serta *informal diplomacy* – misalnya SID pernah terlibat negosiasi krisis sandera *Laju* (1974) dan mendukung upaya menjalin hubungan pasca-konflik dengan Indonesia di akhir 1960-an[6][7].
- Military Intelligence (SAF Intelligence) – Digital and Intelligence Service (DIS): Intelijen militer Singapura dulunya dikelola dalam Military Intelligence Organisation (MIO) di lingkungan Angkatan Bersenjata Singapura (SAF). Pada Oktober 2022, sebagai bagian modernisasi *Next-Gen SAF*, Singapura mengonsolidasi fungsi intelijen militer dan pertahanan siber ke dalam satu matra baru bernama Digital and Intelligence Service (DIS)[8]. DIS menjadi cabang keempat SAF (setara Angkatan Darat, Laut, Udara), bertugas "mempertahankan dan mendominasi domain digital" dalam operasi pertahanan[9]. Di bawah DIS, bernaung:

- *Joint Intelligence Directorate (JID)* yang merumuskan doktrin dan integrasi intelijen-operasi SAF [10].
- *Joint Intelligence Command (JIC)* yang menyediakan intelijen taktis dan strategis bagi MINDEF/SAF serta melatih petugas intelijen militer (meliputi satuan *Imagery Support Group* dan *Counter-Terrorism Intelligence Group*)[11].
- *Cyber Staff* dan *SAF C4 Command* yang menangani keamanan siber pertahanan serta jaringan *Command, Control, Communications, Computers (C4)*[12].
- *Digital Defence Command (DDC)* yang mengembangkan kapabilitas *electronic protection* dan *psychological defence* (pertahanan psikologis) untuk menghadapi ancaman perang elektronik dan informasi[13].
- *Digital Ops-Tech Centre* serta *Training Command* untuk inovasi teknologi (data science, AI) dan pengembangan SDM intelijen-siber[14][15].

Pendirian DIS mencerminkan peningkatan fokus Singapura pada ancaman di ranah siber dan kebutuhan integrasi intelijen dengan operasi militer. DIS memperkuat kemampuan SIGINT elektronik dan *cyber warfare* SAF, sekaligus memastikan interoperabilitas digital di seluruh matra[8][9].

Koordinasi Antarlembaga: Mulai 2004, Singapura membentuk *National Security Coordination Secretariat* (NSCS) di bawah Kantor PM untuk meningkatkan koordinasi kebijakan dan intelijen antara lembaga-lembaga tersebut[16]. NSCS dipimpin seorang Permanent Secretary bidang *National Security & Intelligence Coordination*, membawahi National Security Coordination Centre (perencanaan kebijakan, penilaian risiko, *horizon scanning*) dan sebuah pusat intelijen gabungan (dahulu Joint Counter Terrorism Centre, kini *National Security Research Centre*)[17][18]. NSCS berfungsi sebagai hub arsitektur keamanan nasional – memastikan ISD, SID, dan intelijen militer saling berbagi informasi dan analisis strategis[16]. Sebelum NSCS berdiri, SID dan ISD bekerja sendiri-sendiri dan enggan berbagi data; setelah 2004, keduanya diwajibkan membuka aliran informasi bersama demi menghadapi ancaman teror baru[19]. Melalui mekanisme NSCS inilah intelijen menjadi terintegrasi dalam

pengambilan keputusan nasional, dengan laporan intelijen strategis rutin ke kabinet dan Komite Keamanan Nasional yang diketuai PM atau Menteri Koordinator Keamanan.

Struktur arsitektur intelijen Singapura: ISD di bawah Kementerian Dalam Negeri (MHA) menangani keamanan domestik; SID di bawah MINDEF namun melapor ke PMO menangani intelijen eksternal; dan SAF Intelligence yang terintegrasi dalam DIS (matra digital baru di SAF). Koordinasi oleh NSCS di Kantor PM memastikan sinergi lintas lembaga[4][19].

Posisi dalam Arsitektur Keamanan Nasional: Intelijen Singapura menempati posisi sentral dalam *"Total Defence"* negara. SID dan ISD bertindak sebagai mata dan telinga strategis pemerintah – SID memberikan peringatan dini geopolitik dan terorisme global kepada pembuat kebijakan, sementara ISD menjaga stabilitas internal dan mendeteksi ancaman dalam negeri[20][21]. Hasil intelijen dari kedua lembaga ini serta dari SAF Intelligence disaring dan disinergikan lewat NSCS untuk mendukung perumusan kebijakan keamanan nasional[22]. Struktur ini mirip *model komunitas intelijen* di mana berbagai agensi berbagi info namun tetap menjaga lingkup tugasnya (domestik vs eksternal), dengan PMO sebagai konduktor. Strategi ini memastikan *intel cycle* (pengumpulan-analisis-diseminasi) berjalan komprehensif, mencakup spektrum ancaman multi-dimensi (militer dan non-militer)[23].

Singapura juga menjaga tingkat kerahasiaan dan kontrol politik yang tinggi atas intelijennya. Hanya segelintir pejabat puncak yang mengetahui detail personel dan operasi SID[24]. Fungsi pengawasan publik atas intelijen relatif minimal dibanding negara demokrasi besar; alih-alih, mekanisme akuntabilitas dipercayakan pada lingkaran kepemimpinan inti. Hal ini dianggap perlu mengingat ukuran Singapura yang kecil menuntut aksi intelijen cepat dan terpadu tanpa birokrasi berbelit, meskipun menimbulkan tantangan seperti keterbatasan *check-and-balance* eksternal.

Ekosistem Pengetahuan dan Think Tank di Singapura

Pilar kekuatan intelijen Singapura tidak hanya terletak pada agensi resminya, tetapi juga pada ekosistem pengetahuan yang mendukung analisis strategi keamanan. Pemerintah Singapura secara aktif memanfaatkan lembaga think tank dan institusi riset domestik untuk memperkaya wawasan intelijen serta membangun *resilience* masyarakat terhadap ancaman keamanan. Beberapa di antaranya yang paling berpengaruh adalah:

- S. Rajaratnam School of International Studies (RSIS): Sebuah sekolah dan think tank di bawah Nanyang Technological University (NTU), yang awalnya didirikan sebagai Institute of Defence and Strategic Studies (IDSS). RSIS dikenal fokus pada kajian pertahanan, terorisme, keamanan non-tradisional, dan kebijakan luar negeri. RSIS menaungi lima pusat riset dan tiga program yang mencakup isu pertahanan, keamanan nasional, dan terorisme[25]. Contohnya, Centre of Excellence for National Security (CENS) di RSIS didedikasikan untuk analisis kebijakan keamanan nasional secara *rigorous* dan *policy-relevant*[26]. CENS meneliti topik seperti keamanan siber, disinformasi, campur tangan asing, ancaman hibrida, hingga polarisasi sosial [27]. Peran RSIS/CENS terasa dalam memberi masukan konseptual bagi kebijakan kontra-terorisme, kontra-radikalisasi, dan *social resilience*. NSCS sendiri secara resmi merujuk CENS sebagai mitra pengetahuan strategis pemerintah dalam isu keamanan nasional[26]. Selain riset, RSIS menyelenggarakan forum strategis seperti Asia-Pacific Programme for Senior National Security Officers (APPSNO) dan Terrorism Analysts' Training Course (TATC), yang mempertemukan pejabat intelijen dan pakar untuk berbagi perspektif. Interaksi ini membantu

memastikan komunitas intelijen Singapura selalu terpapar perkembangan teori dan praktik terbaru di bidang keamanan.

- Institute of Southeast Asian Studies – Yusof Ishak Institute (ISEAS): Think tank terkemuka yang didedikasikan pada studi politik, keamanan, dan ekonomi Asia Tenggara. ISEAS berperan memantau tren regional – termasuk dinamika politik negara tetangga, gerakan ekstremis, dan hubungan kekuatan besar di Asia Tenggara. Publikasi ISEAS mengenai politik domestik Indonesia, Malaysia, atau perkembangan di Laut Cina Selatan kerap menjadi sumber acuan analisis bagi intelijen Singapura. Dengan misinya "mendedikasikan diri pada studi tren sosio-politik, keamanan, dan ekonomi di Asia Tenggara"[28], ISEAS membantu *early warning* dan pemahaman konteks bagi pembuat kebijakan Singapura dalam merespons isu kawasan. Misalnya, dalam isu Foreign Terrorist Fighters pasca-ISIS, ISEAS mengkaji pola pergerakan dan upaya deradikalisasi di Indonesia/Filipina[29][30] – pengetahuan ini bermanfaat bagi ISD dan SID dalam merancang strategi mencegah spillover ancaman teroris ke Singapura. Selain itu, ISEAS dan RSIS berkontribusi pada diplomasi jalur kedua (track-two diplomacy) melalui dialog regional yang sering melibatkan mantan pejabat intelijen atau militer.
- Centre of Excellence for National Security (CENS): Secara khusus, CENS layak disorot karena posisinya yang unik: didirikan pasca-September 11 untuk meneliti *non-traditional security* dan berada dalam orbit RSIS–PMO. CENS sering mengadakan lokakarya terkait ancaman terorisme, *cyber threats*, *foreign influence*, dan bahkan *social media analytics* untuk keamanan. Kajiannya membantu intelijen memahami fenomena "radikalisasi online", strategi kontra-narasi, hingga teknik *horizon scanning* ancaman non-konvensional. Pemerintah kerap mengundang peneliti CENS dalam merumuskan kebijakan semisal RUU *Foreign Interference (Countermeasures) Act (FICA)* 2021 yang bertujuan menangkal campur tangan asing di domain informasi[31]. Dengan demikian, think tank seperti CENS menjadi *brain trust* yang melengkapi kapasitas analisis intelijen formal.
- Nanyang Technological University (NTU) dan National University of Singapore (NUS): Selain think tank, komunitas akademik di universitas Singapura juga mendukung ekosistem intelijen. Program studi hubungan internasional, kajian strategis, sains data, hingga bahasa asing mencetak calon analis dan agen intelijen berkualitas. Banyak staf intelijen direkrut dari lulusan terbaik universitas lokal (lihat bagian SDM). Bahkan ada skema di mana mahasiswa tingkat akhir diundang dalam "tea session" tertutup oleh SID untuk menjaring minat bergabung[32]. Kolaborasi riset antara lembaga keamanan dan akademisi juga umum – misal DSO National Labs (lembaga R&D pertahanan) bermitra dengan NTU dalam riset AI keamanan[33].

Secara keseluruhan, ekosistem pengetahuan Singapura bersifat terpadu dengan sistem intelijen. Ada *integrated feedback loop*: Think tank memberikan analisis dan skenario alternatif, pemerintah menyuplai dukungan dana/akses data, dan hasil kajian diintegrasikan dalam strategi nasional. Model ini memperkaya perspektif intelijen (agar tidak silo) serta membantu menghindari *groupthink*. Bahkan pejabat tinggi seperti PM Lee kerap mengutip hasil think tank dalam pidato kebijakan luar negeri. Keberadaan think tank kuat juga meningkatkan *soft power* Singapura, karena narasi dan ide strategis yang dihasilkan (contoh: konsep ASEAN centrality, kontra-terorisme komprehensif) bergaung di tingkat regional dan mengukuhkan posisi intelijen Singapura sebagai pemasok *insight* berkualitas di Asia Tenggara.

Aliansi Strategis dan Kolaborasi Internasional

Kekuatan intelijen Singapura turut ditopang oleh jaringan aliansi strategis dan kolaborasi dengan negara sahabat, terutama dalam hal teknologi, cyber intelligence, dan interoperabilitas regional. Dalam 10 tahun terakhir, Singapura semakin proaktif menjalin kerja sama intelijen dengan kekuatan besar maupun negara regional untuk memperkuat daya deteksi dan daya gentarnya:

- Hubungan dengan Amerika Serikat: AS memandang Singapura sebagai mitra strategis dan *reliable* di Asia[34]. Keduanya mempunyai *Defence Cooperation Agreement* dan berbagai nota kesepahaman di bidang keamanan. Intelijen Singapura secara rutin berbagi informasi kontra-terorisme dengan AS sejak era pasca-9/11. Misalnya, setelah pengungkapan rencana JI untuk mengebom Kedubes AS dan fasilitas lain di Singapura 2001, intel Singapura bekerja erat dengan agen AS (CIA, FBI) untuk melacak jaringan regional[35][18]. Dalam ranah teknologi, terbaru pada Juli 2024 Departemen Pertahanan AS dan Kementerian Pertahanan Singapura menandatangani *Statement of Intent* baru untuk kerja sama data analytics dan artificial intelligence (AI)[36]. Langkah ini bertujuan memperkuat *interoperability* antara sistem analitik intelijen kedua negara serta memastikan penggunaan AI yang *bertanggung jawab*[37]. Singapura juga tergabung dalam latihan-latihan intelijen multinasional yang dipimpin AS, dan menjadi peserta aktif Five Eyes plus forum (walau bukan anggota Five Eyes, Singapura sering diundang berbagi intel dalam isu tertentu seperti terorisme). Indikasi kolaborasi mendalam terlihat dari bocoran tahun 2013 yang menyebut SID bekerja sama dengan Australian Signals Directorate dan NSA dalam operasi penyadapan kabel internet bawah laut regional[38]. Operasi rahasia ini menunjukkan Singapura berkontribusi dalam jaringan SIGINT global pimpinan AS-Australia, memanfaatkan posisi geografisnya yang strategis di jalur komunikasi internasional. Selain itu, militer Singapura mengikuti latihan siber bilateral dengan US Cyber Command, dan kedua negara saling menempatkan perwira penghubung (*liaison officers*) di pusat fusi intelijen regional.
- Kerja Sama dengan Inggris: Hubungan intelijen Singapura-Inggris berakar dari sejarah (warisan intelijen kolonial Special Branch) dan kini diperkuat kemitraan strategis baru. September 2023, PM Lee Hsien Loong dan PM Rishi Sunak menandatangani Joint Declaration of Strategic Partnership yang mencakup pilar khusus “Kerja Sama Pertahanan, Keamanan, *Intelligence*, dan Kebijakan Luar Negeri”[39]. Ini menandai secara resmi diakuinya dimensi intelijen dalam hubungan bilateral. Kolaborasi praktisnya antara lain: Inggris dan Singapura memperdalam kemitraan siber, misalnya program pertukaran informasi ancaman siber, latihan bersama penanganan *hybrid threats*, dan berbagi keahlian dalam Digital and Intelligence Service (DIS) yang baru dibentuk Singapura[40]. Inggris juga mendukung peningkatan kapabilitas AI Singapura secara global – November 2024, Singapura-UK meneken MoC tentang keselamatan AI dan interoperabilitas teknologi digital[41]. Dalam domain tradisional, intelijen militer kedua negara sudah lama bekerjasama di bawah kerangka Five Power Defence Arrangements (FPDA) yang mencakup UK, meski FPDA fokus pertahanan, ia melibatkan pertukaran intelijen pengawasan maritim dan udara untuk pertahanan Malaysia-Singapura. Singapura mendapat manfaat dari pengalaman luas Inggris di counter-intelligence (MI5) dan counter-terrorism (MI6), sementara Inggris memanfaatkan pemahaman mendalam Singapura atas dinamika Asia Tenggara.
- Hubungan erat dengan Australia: Australia adalah mitra intelijen kunci, terlihat dari kerja sama SIGINT tadi serta status Australia sebagai salah satu *closest defence partners*. Intel Singapura dan Australia saling berbagi info *real-time* tentang pergerakan teroris di Asia Tenggara (contoh: pertukaran data soal warga Asia Tenggara anggota ISIS di Suriah). Pada 2018, Singapura bergabung dalam prakarsa “Our Eyes” yang diprakarsai Indonesia dan didukung Australia – sebuah platform *intelligence sharing* di ASEAN untuk memantau teroris lintas negara[42]. Australia menyokong platform ini secara teknologi dan pelatihan. Selain itu, di sektor *cyber*

intelligence, Singapura dan Australia menandatangani kesepakatan *Cyber Cooperation Program* yang meliputi latihan tanggap insiden siber regional. Posisi Singapura sebagai tuan rumah Information Fusion Centre (IFC) maritim dan Counter-Terrorism Information Facility (CTIF) (lihat bagian selanjutnya) juga melibatkan keikutsertaan perwira Australia. Fakta bahwa Australian Signals Directorate (ASD) bersama SID melakukan operasi penyadapan kabel bawah laut[43] mengindikasikan tingkat saling percaya yang tinggi – operasi tersebut bagian dari program intelijen sinyal global dan Singapura dianggap cukup andal untuk diajak bekerja sama pada materi sangat sensitif.

- Kemitraan pertahanan-intelijen dengan Israel: Hubungan Singapura-Israel terjalin sejak awal kemerdekaan Singapura, ketika Israel membantu melatih SAF. Sepuluh tahun terakhir, kolaborasi berfokus pada teknologi intelijen dan siber. Singapura menjadi salah satu pasar kunci bagi perusahaan *cyber intelligence* Israel. Laporan tahun 2019 menyebut Singapura kembali mengontrak perusahaan *cyber espionage* Israel untuk kemampuan *interception* dan analisis siber canggih[44][45]. Hal ini terjadi setelah skandal spyware Pegasus; Singapura mencari solusi baru dari firma Israel lain yang kurang terpublikasi. Interaksi intel resmi juga ada – misalnya pelatihan bersama unit *signals intelligence* Singapura dengan Unit 8200 (intelijen sinyal IDF) secara tertutup. Keduanya menghadapi ancaman siber serius, sehingga Cyber Security Agency (CSA) Singapura menjalin nota kesepahaman dengan Israel National Cyber Directorate untuk bertukar *best practices* dan melakukan *joint cyber drills*[46]. Pada tataran strategis, Singapura dan Israel rutin berdialog mengenai ancaman ekstremisme (berbagi pembelajaran penanggulangan lone-wolf attacks, dsb.). Israel juga memasok peralatan intelijen canggih ke Singapura, mulai drone pengintaian, sistem radar ELINT, hingga software analitik big data. Sebaliknya, Singapura menjadi *hub* bagi perusahaan teknologi keamanan Israel untuk ekspansi ke Asia Tenggara[47]. Aliansi tak resmi namun erat ini memberi Singapura keunggulan teknologi dibanding negara ASEAN lain, sementara bagi Israel, Singapura adalah pintu masuk pasar dan mitra intel terpercaya di Asia.
- Kerja sama regional ASEAN dan negara tetangga: Selain aliansi dengan kekuatan besar, Singapura aktif mendorong interoperabilitas intelijen di tingkat regional. Sebagai contoh, Singapura terlibat penuh dalam forum intelijen ASEAN seperti ASEANAPOL Intelligence Exchange dan platform *counter-terrorism information sharing* di bawah ASEAN Defence Ministers' Meeting (ADMM)-Plus. Inisiatif "ASEAN Our Eyes (AOE)" yang dimulai 2018 melibatkan Singapura bersama Indonesia, Malaysia, Thailand, Brunei, Filipina untuk saling bertukar *dossier* teroris lintas negara[42]. Meski implementasinya menghadapi kendala birokrasi di beberapa negara[48], Singapura mendorong agar AOE efektif – bahkan mendirikan Counter-Terrorism Information Facility (CTIF) yang dapat dilihat sebagai platform pelengkap AOE (dengan melibatkan juga mitra seperti Australia, AS, dll). Dengan Indonesia dan Malaysia, intel Singapura menjalin komunikasi erat khususnya dalam pengawasan pergerakan militan di kawasan Selat Malaka dan perbatasan. Walaupun pernah ada sensitivitas (misal insiden masa lalu ketika intel Singapura dituduh memata-matai Malaysia), dekade terakhir hubungan intelijen bilateral membaik karena ancaman bersama (ISIS, radikalisme). Singapura juga anggota *"Triad"* intelijen informal bersama Malaysia dan Australia untuk berbagi info *real-time* soal pejuang asing kembali (FTF returnees). Di lingkup Five Power Defence Arrangements (FPDA), Singapura berperan dalam integrasi gambaran radar dan maritime domain awareness bersama Malaysia, Australia, NZ, UK – melibatkan *fusion* data intel guna mendeteksi ancaman udara/maritim di sekitar Semenanjung Malaya.

Interoperabilitas Regional: Sebagai pusat logistik militer AS dan tuan rumah berbagai pusat informasi, Singapura memfasilitasi *interoperability* intelijen kawasan. Contoh konkret adalah pendirian Counter-Terrorism Information Facility (CTIF) di Pangkalan Changi. CTIF diluncurkan Januari 2021 dan diresmikan Menhan Ng Eng Hen pada September 2022[49][50]. CTIF merupakan fasilitas multilateral lintas instansi yang mengumpulkan negara "sehaluan" untuk berbagi intel dan peringatan dini terorisme regional[51]. Meskipun banyak operasinya dirahasiakan, CTIF krusial mensinergikan upaya kontra-teror kawasan melalui intelijen kolektif dan metode berbasis data[51]. Sejak beroperasi, CTIF telah menghasilkan produk intelijen tepat waktu bersama negara mitra dan membantu aksi kolektif kawasan melawan teror[50]. Menariknya, jabatan kepala CTIF bersifat bergilir; pada 2023 perwira Filipina memimpin CTIF[52], menandakan kepercayaan kawasan terhadap Singapura sebagai *honest broker*. Selain CTIF, Information Fusion Centre (IFC) yang didirikan RSN (TNI AL Singapura) pada 2009 adalah pusat fusi maritim yang melibatkan 24 negara dengan perwira penghubung ditempatkan di Singapura[53]. IFC telah berhasil menurunkan insiden perompakan di Selat Malaka/Singapura hingga 92% periode 2015-2018 dengan menyediakan info aksi bersama angkatan laut regional[54][55]. Contohnya, IFC membantu TNI-AL menangkap kapal *MV Sunrise Glory* (penyelundup narkotika) dengan berbagi data pelacakan selama 3 bulan[56][57]. Ini menunjukkan intelijen Singapura menjadi *enabler* keamanan kolektif, meningkatkan pengaruh Singapura di ASEAN lewat peran "pemasok informasi kritis" bagi negara-negara tetangga.

Kolaborasi internasional ini membawa manfaat timbal balik: Singapura memperoleh akses intelijen global yang lebih luas dan teknologi mutakhir, sedangkan mitra asing mendapat jaringan regional andal melalui Singapura. Hubungan saling percaya yang terjalin – misalnya AS menyebut Singapura "mitra pertahanan paling bernilai" di Indo-Pasifik[58][59] – memperkokoh posisi intelijen Singapura sebagai kekuatan yang jauh melebihi ukurannya.

Teknologi dan Inovasi Intelijen

Dekade terakhir, Singapura menginvestasikan sumber daya besar untuk memodernisasi teknologi intelijen. Fokusnya pada penguatan kemampuan *Signals Intelligence (SIGINT)*, *Cyber Intelligence*, pemanfaatan *Big Data* dan *Artificial Intelligence (AI)*, serta integrasi sistem intelijen nasional. Beberapa capaian dan inisiatif utama:

- Transformasi Digital Intelijen Militer (DIS): Seperti diuraikan, pembentukan Digital and Intelligence Service (DIS) tahun 2022 menjadi tonggak inovasi. Dengan DIS, Singapura kini memiliki *dedicated cyber command* dalam militer, yang menggabungkan unit-unit SIGINT, *cyber defence*, perang elektronik, hingga *psyops*. Ini memungkinan respon terpadu terhadap ancaman hibrida. SIGINT Singapura diperkuat melalui integrasi kemampuan intersepsi dan *surveillance* di DIS – baik itu penyadapan komunikasi, pemantauan spektrum elektromagnetik, maupun *geospatial intelligence* (melalui Imagery Support Group)[11]. Selain itu, DIS membangun Digital Ops-Tech Centre yang melatih personel dalam *data science* dan AI untuk analisis intelijen yang lebih mendalam[14]. Artinya, analisis big data – entah dari *open-source intelligence (OSINT)* seperti media sosial maupun dari sensor militer – kini menjadi bagian inti ekosistem intelijen Singapura. Kapabilitas *machine learning* diterapkan untuk mendeteksi pola terorisme (contoh: pola transaksi keuangan mencurigakan atau jejak digital propaganda ekstremis). DIS juga meluncurkan pusat AI militer tahun 2024 untuk mengembangkan teknologi seperti komputasi awan militer dan 5G[60]. Ini *blueprint* menuju militer yang mengandalkan kecerdasan buatan dalam pengambilan

keputusan taktis. Di latihan terbaru, prajurit SAF diuji coba menggunakan AI *speech-to-text* untuk input perintah secara hands-free saat memegang senjata[61] – inovasi kecil ini bisa punya implikasi besar bagi intel di lapangan (misal, pencatatan laporan intel lewat suara). Singapura pun terlibat aktif dalam menyusun norma global etika AI militer, dengan ikut menyelenggarakan Responsible AI in Military Domain Summit 2024 dan mengajukan resolusi PBB untuk penggunaan AI yang aman[62]. Ini menunjukkan Singapura ingin memimpin, bukan sekadar mengikuti, dalam pemanfaatan AI di keamanan.

- Kemampuan *Cyber Intelligence* dan Keamanan Siber: Sebagai negara paling terhubung digital di Asia Tenggara, Singapura membangun kapabilitas intelijen siber yang unggul. Tahun 2015 dibentuk Cyber Security Agency (CSA) tersendiri, yang meski fokusnya perlindungan infrastruktur kritikal, juga bekerja erat dengan ISD/SID untuk deteksi ancaman siber. *Joint Cyber Staff* di DIS kini mengoordinasikan kebijakan *cyber defence* seantero sektor pertahanan, menyusun strategi, dan mendukung CSA bila diperlukan[63]. Singapura menggelar latihan siber lintas instansi (Critical Infrastructure Defence Exercise – CIDeX) yang melibatkan CSA dan DIS melatih kementerian lain menghadapi serangan siber[64]. Intelijen siber juga diperkuat melalui kolaborasi internasional: misalnya, Singapura menggagas ASEAN Cyber Capacity Program, dan menjalin aliansi teknis dengan negara maju (AS, Israel, Inggris seperti dijelaskan) untuk bertukar *threat intelligence feeds* (indikator serangan, teknik peretasan terkini). Hasilnya, Singapura berhasil merespon beberapa ancaman siber regional. Contoh: ISD mendeteksi upaya kelompok hacker terkait negara untuk mencuri data riset COVID-19 di kawasan, dan berbagi peringatan dengan tetangga. Di ranah *offensive cyber*, meski detailnya tertutup, dapat diduga intelijen Singapura memiliki *cyber espionage unit* yang sanggup mengakses target di wilayah prioritas (contoh: memantau pergerakan militer atau kelompok teroris melalui peretasan komunikasi). Kabar bahwa Singapura memakai perangkat *spyware* canggih dari perusahaan Israel[44][45] memperkuat anggapan adanya *offensive cyber capability* untuk kepentingan keamanan nasional (misalnya memantau tersangka teroris di platform terenkripsi).
- Integrasi *Big Data Analytics*: Intelijen modern ditandai *data-driven approach*. Singapura mengerahkan teknologi *big data* untuk mengolah volume informasi besar secara cepat. Dalam konteks kontra-terorisme, SID mengakui misi agensi meluas mencakup analisis perkembangan global apa pun yang bisa berdampak ke Singapura[65]. Ini mencakup misal *real-time analytics* terhadap media sosial global terkait sentimen anti-Singapura atau narasi ekstremis. CTIF menggunakan *data-driven methods* untuk mendeteksi penyebaran ideologi ekstremis di kawasan secara dini[51][66]. Salah satu pencapaian yang disebut Menhan Ng adalah CTIF berhasil mengendus tren penyebaran ideologi radikal online sebelum berbuah aksi, sehingga aparat regional bisa bertindak mencegah[66]. Hal ini dimungkinkan lewat pemanfaatan analitik data (misal, memonitor grup Telegram radikal, menganalisis kata kunci). Pada tataran domestik, pemerintah meluncurkan proyek National AI Programme di sektor keamanan (bagian dari proyek AI Nasional) yang salah satunya berfokus pada keamanan perbatasan dan deteksi ancaman otomatis[67]. Singapura juga bekerja dengan Departemen Pertahanan AS dalam mempercepat adopsi analitik data – Juli 2024 ditandatangani MoU inovasi pertahanan agar kedua negara dapat mencari teknologi canggih secara cepat dan efektif[68]. Melalui nota ini, Singapura berpeluang mengakses solusi AI AS untuk intelijen (misal analisis citra satelit otomatis, deteksi anomali jaringan). Pada saat bersamaan, Singapura mengadopsi pendekatan *whole-of-government* dalam teknologi: DSTA (Defence Science & Technology Agency) mendorong adaptasi teknologi komersial untuk militer karena biaya lebih rendah dan inovasi cepat[69]. Sebagai contoh, memanfaatkan *cloud computing* komersial yang aman untuk mempercepat sharing intel

antarlembaga[70].

- Surveilans Berbasis Smart Technology: Menjadi negara kota padat, Singapura memanfaatkan inisiatif Smart Nation untuk mendukung intelijen. Jaringan kamera CCTV cerdas dan sensor IoT ditempatkan di ruang publik yang bisa diakses aparat keamanan untuk memonitor potensi ancaman (dengan analitik video otomatis mendeteksi perilaku mencurigakan). Program seperti Safe City testbed melibatkan integrasi data dari kamera, drone, dan unit patroli, memberikan situational awareness tinggi kepada ISD dan kepolisian. Hal ini penting dalam kontra-teror dan kontra-intelijen: misal, bisa melacak pergerakan agen asing atau pengintaian teroris secara *real-time*. Meski tak dipublikasikan detailnya, kemungkinan Singapura telah menguji sistem pengenalan wajah (facial recognition) skala nasional untuk penegakan hukum. Keseimbangan pun dijaga dengan kebijakan perlindungan data ketat agar tidak ada penyalahgunaan.

Singkatnya, Singapura berusaha berada di garis depan inovasi intelijen di Asia Tenggara. Dengan mengawinkan kapabilitas teknologi mutakhir dan pengembangan SDM (lihat bagian SDM), intelijen Singapura mampu menghadapi ancaman “high-tech” seperti *cyberterrorism*, spionase siber, dan propaganda online. Tantangan ke depan adalah memastikan integrasi mulus antar sistem (militer-sipil), serta menjaga pertumbuhan teknologi ini tetap *secure & ethical*. Sejauh ini, Singapura menunjukkan keseriusan di keduanya – baik lewat investasi teknis maupun terlibat dalam inisiatif tata kelola AI global [62].

Strategi Rekrutmen dan Penguatan SDM Intelijen

Sumber daya manusia (SDM) yang unggul adalah fondasi kekuatan intelijen Singapura. Dengan populasi hanya ~5,5 juta, Singapura menghadapi tantangan keterbatasan SDM, namun mengatasinya melalui rekrutmen selektif, pelatihan intensif, serta pemanfaatan skema wajib militer (*National Service*) untuk menjaring talenta. Strategi SDM intelijen dalam 10 tahun terakhir menonjol dalam hal berikut:

- Rekrutmen Jalur Sipil (Profesional): Lembaga seperti SID dan ISD merekrut staf sipil profesional baik fresh graduate maupun *mid-career*. Tradisinya, SID dulu merekrut diam-diam dari lulusan terbaik universitas melalui undangan *“tea session”* eksklusif[71]. Pola ini berubah seiring waktu. Pada 19 Juli 2021, SID untuk pertama kalinya meluncurkan website resmi dan membuka proses rekrutmen secara publik[72]. Langkah ini bertujuan menjaring beragam latar belakang talenta Singapura yang mungkin sebelumnya tidak terjangkau[73]. Seorang direktur SID, disamarkan sebagai “Michael”, menjelaskan bahwa ancaman kian kompleks sehingga SID butuh spektrum keahlian lebih luas[74]. Kini SID aktif mencari kandidat dengan latar ekonom, pengacara, pakar keuangan, ilmuwan data, selain spesialis wilayah/bahasa[75]. Bahkan SID telah menerima seorang mantan bankir untuk membantu analisis sistem finansial terorisme[76]. Ini menunjukkan pergeseran dari fokus hanya *generalist* lulusan ilmu politik, menjadi multidisipliner. Pembukaan situs juga berfungsi mengikis miskonsepsi publik—SID menegaskan kerja intelijen tak se-“glamor” di drama TV dan bukan berarti mengorbankan kehidupan pribadi sepenuhnya[77]. Kampanye publik ini membidik membangun citra bahwa karier intelijen *“meaningful, intellectual, yet patriotic”*, sehingga orang berbakat tertarik bergabung demi *sense of purpose* melindungi negara[78].
- Diversifikasi dan Pencegahan *Groupthink*: SID secara eksplisit menyatakan perlunya *diverse perspectives* agar tidak terjebak *groupthink*[79][80]. “Michael” menyebut SID sengaja mendorong debat internal dan “creative tension” dalam organisasi[81]. Untuk itu, merekrut SDM dari berbagai latar (sosial-budaya, pendidikan, gender) menjadi strategi. Jumlah analis wanita pun meningkat,

contohnya seorang analis “Sophie” menceritakan pengalaman 8 tahun di SID dengan banyak kesempatan pengembangan (belajar bahasa asing tambahan, pelatihan analisis data)[82][83]. Organisasi melatih anggota agar mampu beradaptasi berbagai peran sepanjang karier – intelijen Singapura bangga membentuk “all-rounded intelligence professional”[84]. Perekrutan juga mencakup program beasiswa intelijen bagi mahasiswa, meski rinciannya dirahasiakan (SID menawarkan internship dan scholarship bagi kandidat potensial, meski info detail hanya diberikan via email kontak rekrutmen)[85]. Langkah ini serupa pola birokrasi Singapura lainnya: menjaring talenta sejak dini, mengikat mereka dengan ikatan dinas, lalu memberi jenjang karier terstruktur. Untuk intelijen, hal ini memastikan kesinambungan kader.

- Pelatihan dan Pengembangan Karier: Begitu bergabung, petugas intelijen Singapura mendapat pelatihan intensif. SID memiliki *People Development Philosophy* dan *Job Families* yang memetakan jalur peningkatan keahlian (analisis, operasi, teknologi, dsb)[86][87]. *Cross-training* antardivisi umum dilakukan agar analis memahami kebutuhan operator, begitu pula sebaliknya. Banyak staf intelijen diberi kesempatan *assignment* luar negeri – entah di kedutaan sebagai *bilateral liaison*, penempatan di pusat intelijen sekutu, ataupun studi lanjut. Mantan Direktur SID dan Presiden S.R. Nathan misalnya pernah ditugaskan di Kedubes Singapura di Washington dalam kapasitas intelijen[88]. Pengalaman internasional ini membangun jejaring dan wawasan global para perwira intelijen. Di tingkat nasional, terdapat Joint Training antara SID, ISD, SAF Intelligence di area seperti analisis terorisme dan kontra-intelijen domestik. Bahkan sebelum NSCS berdiri, Singapura punya Joint Intelligence School (non-publik) untuk melatih agen dari berbagai agensi secara bersama. Sekarang, dengan DIS Training Command akan didirikan (2023)[89], pelatihan intelijen militer makin terstruktur, meliputi sekolah intelijen dan siber dalam SAF.
- Peran *National Service* (Wajib Militer): National Service (NS) adalah kewajiban pria Singapura berusia 18 tahun untuk bertugas ~2 tahun di militer, kepolisian, atau pertahanan sipil. Singapura melihat NS bukan hanya pemenuh kebutuhan militer, tetapi juga sarana menyaring bakat siber dan intelijen. Tahun 2018, MINDEF meluncurkan Cyber NSF Scheme – program inovatif menempatkan pemuda berkemampuan IT tinggi dalam unit siber SAF selama NS mereka[90]. Para *Cyber NSF* ini melalui seleksi ketat (tes kriptografi, keamanan jaringan, dll) dan jika lolos mereka mendapat Cyber Specialist Award[90][91]. Program tersebut menggabungkan tugas operasional (misal: *incident response*, *malware analysis*, *penetration testing*) dengan pendidikan akademik *Work-Learn Programme* di universitas lokal selama 3-4 tahun[92][93]. Singapura menggandeng Singapore Institute of Technology (SIT) dan NUS untuk memberikan modul kuliah bagi Cyber NSF, yang kreditnya diakui menuju gelar S1 di bidang keamanan siber[92][94]. Hasilnya, hingga 2020 sekitar 170 pemuda terpilih telah mengikuti skema ini dan bergabung dengan unit siber pertahanan[95][96]. Mereka lulus dari kursus spesialis siber (35 minggu) dan langsung ditempatkan menjaga jaringan MINDEF/SAF dari peretasan[97]. Para lulusan angkatan pertama (2019) menjadi bagian penting tenaga ahli siber muda di pertahanan Singapura[98]. Selain siber, NS menyalurkan juga bakat ke intelijen militer tradisional: contohnya C4 Expert (C4X) vocation untuk teknisi jaringan dan Defence Cyber Expert (DCX) untuk staf siber non-militer[99]. Dengan begini, NS tidak lagi dipandang sebagai *wasted time* tetapi sebagai *talent pipeline*. Setelah NS, banyak dari spesialis ini direkrut sebagai pegawai tetap MINDEF, memperkuat komunitas intelijen jangka panjang.
- Jalur Militer Reguler: Terlepas dari NS, intelijen militer juga diperkuat lewat karier reguler di SAF. Kini ada korps perwira intelijen di SAF yang setara korps tempur. Pembentukan DIS memperjelas jenjang karier: jabatan Chief of Digital and Intelligence Service (CDI) menjadi posisi bintang-2

baru di SAF[100], membuka aspirasi bagi perwira muda meniti karier di intelijen. Akademi militer (SAFTI) memasukkan kurikulum peperangan siber dan intelijen dasar untuk semua calon perwira. Ini penting agar *mindset* intelijen tertanam di seluruh jajaran komando.

Melalui kombinasi strategi di atas, Singapura berupaya memastikan intelijen selalu diisi personel terbaik. Kecilnya populasi diatasi dengan *head-hunting* agresif dan pengembangan internal jangka panjang. Penggunaan NS sebagai pengungkit membuahkan *keunggulan kuantitas dan kualitas SDM siber* dibanding negara tetangga (yang umumnya tidak punya program serupa). Tentu, ada tantangan seperti mempertahankan kerahasiaan identitas agen di negara yang masyarakatnya saling kenal – namun SID mengatur itu dengan baik (pegawai SID umumnya mengaku bekerja di MINDEF dengan alasan “pekerjaan sensitif” kepada kerabat[101]).

Akhir dekade ini, intelijen Singapura semakin *“millennial-friendly”*: lebih terbuka merekrut lewat internet, menawarkan *work-life balance* relatif (ditegaskan bahwa kerja di SID “tidak berbahaya seperti asumsi publik”[77]), dan menggaet semangat patriotisme generasi muda. Ini langkah antisipatif agar generasi berikutnya tetap mau bergabung di tengah persaingan sektor teknologi swasta yang juga menarik minat talenta digital.

Aktivitas Regional dan Pengaruh Intelijen Singapura di Asia Tenggara

Sebagai negara kecil di jantung Asia Tenggara, Singapura memikul kepentingan vital untuk stabilitas kawasan. Intelijen Singapura karenanya sangat aktif dalam beragam aktivitas keamanan regional, mencakup kontra-terorisme, keamanan maritim, hingga perang informasi. Berikut sorotan peran dan pengaruhnya, termasuk terhadap Indonesia dan negara ASEAN lain:

- Kontra-Terorisme Regional: Singapura termasuk pionir dalam upaya regional melawan terorisme Jihadis sejak awal 2000-an. Setelah serangan 9/11, ISD membongkar sel Jamaah Islamiyah (JI) Singapura pada 2001, menangkap belasan anggota serta menggagalkan rencana pengeboman sejumlah target (Kedubes AS, fasilitas militer, stasiun MRT)[102]. Sebagian tersangka kabur ke luar negeri (Malaysia, Indonesia) – intelijen Singapura lalu melancarkan operasi multi-agency bersama mitra ASEAN untuk memburu mereka[103]. Michael (SID) menyebut keberhasilan operasi ini adalah mampu memberikan peringatan dini kepada mitra atau pemerintah Singapura tentang ancaman teroris sebelum serangan terjadi[104]. Salah satu buronan JI, Mas Selamat Kastari, ditangkap di Johor 2009 berkat koordinasi intel Singapura-Malaysia. Dalam dekade terakhir, ancaman ISIS muncul dan Singapura kembali proaktif: tahun 2016 intelijen Singapura membantu Indonesia menggagalkan rencana serangan kelompok Batam terhadap Marina Bay Sands. Kasus ini melibatkan sekelompok militan di Batam yang berencana menembakkan roket ke Singapura; ISD/SID mendeteksi komunikasi mereka dan berkoordinasi dengan Densus 88 Polri untuk menangkap para pelaku sebelum rencana berjalan[105]. Demikian pula, Singapura waspada terhadap warga regional yang pulang dari Suriah – ISD berbagi info *watchlist* FTF dengan Malaysia dan Indonesia. Singapura juga menyumbang keahlian deradikalisasi: program Religious Rehabilitation Group (RRG) Singapura (kelompok ulama mendampingi tahanan teror) menjadi model acuan bagi negara tetangga.
- Fasilitator Platform Intelijen Multilateral: Intelijen Singapura meningkatkan pengaruhnya dengan menjadi tuan rumah fasilitas intelijen bersama. Counter-Terrorism Information Facility (CTIF) di

Changi yang melibatkan perwira dari berbagai negara (ASEAN, plus Australia, NZ, dll) adalah contoh nyata. CTIF menyediakan wadah analisis bersama, memungkinkan tiap negara memperoleh gambaran ancaman kawasan yang komprehensif. Sejak operasional 2021, CTIF telah menghasilkan intelijen tepat waktu yang mendorong aksi kolektif[50]. Misalnya, CTIF mengidentifikasi peningkatan propaganda pro-ISIS di Asia Tenggara di ranah online, lalu berkoordinasi dengan otoritas Malaysia-Filipina untuk menindak kelompok penyebar, sehingga potensi serangan dapat dicegah – hal ini disinggung Menhan Ng bahwa CTIF mendeteksi penyebaran ideologi ekstremis hingga direspons aparat regional[66]. Kesuksesan CTIF membawa prestise bagi Singapura sebagai leader intelijen regional. Selain CTIF, di domain maritim, Information Fusion Centre (IFC) telah diakui dunia sebagai model pusat informasi maritim. Dengan menempatkan 19 perwira asing secara permanen di IFC[106][107], Singapura membangun jejaring intelijen maritim global. IFC tak hanya berbagi data, tetapi juga melatih kebiasaan berbagi informasi antar negara yang sebelumnya enggan (membangun *trust*). Hasil nyata: penurunan drastis aksi perompakan di Selat Malaka (dari 104 kasus pada 2015 menjadi hanya 8 kasus tahun 2018) sebagian besar dikreditkan pada kolaborasi yang diorkestrasi IFC[54][55]. *Track record* positif ini memperkuat posisi Singapura di forum maritim ASEAN dan IMO, memberi bobot diplomatik dalam isu keamanan laut.

- Keterlibatan Intelijen di Isu Perbatasan dan Maritim: Singapura berkepentingan menjaga keamanan selat dan perbatasan maritimnya yang sempit dengan Indonesia dan Malaysia. Intelijen Singapura memantau ketat pergerakan di Selat Singapura dan Johor. Salah satu atensi besar adalah penyelundupan (senjata, narkoba, migran) yang bisa menimbulkan instabilitas. Contoh pada Februari 2018, IFC bersama intelijen Singapura melacak kapal *MV Sunrise Glory* selama 3 bulan, curiga kapal itu terlibat penyelundupan narkoba lintas selat[56]. Info intel ini dibagikan via perwira penghubung Indonesia di IFC, sehingga TNI AL berhasil mencegat kapal tersebut dan menemukan 1 ton sabu di dalamnya[108]. Demikian pula dalam kasus kapal *Hai Soon 12* yang dibajak perompak Mei 2016 – IFC menggunakan tracker GPS cadangan untuk menemukan kapal dan memberi koordinat ke TNI AL yang kemudian menyelamatkan kapal beserta 21 ABK tanpa korban[109]. Ini memperlihatkan pengaruh informasi Singapura: kemampuan mengumpulkan data (melalui jaringan AIS, radar, intel satelit) dan mendistribusikannya secara efektif, sehingga negara tetangga terbantu menegakkan keamanan di wilayahnya. Dalam konteks sengketa maritim (seperti isu batas laut dengan Malaysia di Tuas atau Pedra Branca), Singapura juga mengandalkan intelijen untuk *early warning* langkah negara lain – misal, memonitor manuver kapal pemerintah asing. Hal ini dilakukan hati-hati agar tidak memperuncing tensi, namun jelas intelijen berperan menyediakan pemahaman situasi yang akurat demi negosiasi diplomatik yang solid.
- Pengaruh pada *Information Operations* dan Opini Publik: Singapura menyadari ancaman "pengaruh informasi" di era *fake news* dan *political warfare*. Maka, intelijen Singapura juga aktif dalam kontra-propaganda dan kontra-pengaruh asing. ISD memiliki unit *Security (Internal) Communications* yang bekerja sama dengan Kementerian Komunikasi dalam mendeteksi dan menepis disinformasi yang disebar aktor asing. Tahun 2017, Singapura menghadapi kasus *"agents of influence"* seperti akademisi Huang Jing yang disebut bekerja untuk kepentingan asing mempengaruhi kebijakan publik Singapura[110]. ISD mengumpulkan bukti interaksinya dengan intel asing dan pemerintah bertindak tegas dengan mengusir Huang Jing serta istrinya pada 2017 [111][112]. Pesan ini bergema di kawasan bahwa Singapura tak mentolerir infiltrasi opini oleh negara asing (banyak yang menduga negara asing tersebut Tiongkok, mengingat Huang sering menulis opini pro-Beijing[113]). Setelah itu, Parlemen Singapura mengesahkan Foreign

Interference Countermeasures Act (FICA) 2021, yang disokong data intelijen tentang modus operandi agen asing di media sosial[114]. Meski FICA menuai kritik dari segi HAM, pemerintah bersikukuh ini perlu demi menutup celah perang informasi. Intelijen Singapura juga proaktif membantu negara tetangga menangkal pengaruh ekstrimis. Misalnya, setelah ledakan hoaks di Malaysia pasca-ISIS, ISD berbagi pengalaman program deradikalisasi dan *counter-messaging* melalui forum regional, yang sedikit banyak memengaruhi kebijakan Malaysia membentuk Unit Countering Violent Extremism.

- Soft Power Intelijen via Think Tank dan Diplomasi: Pengaruh intelijen Singapura tidak selalu *coercive*; kadang muncul halus melalui produksi wacana strategis. Contohnya, RSIS sering menerbitkan *commentary* mengenai keamanan regional yang dibaca luas oleh elit ASEAN. Semisal commentary tentang perlunya *"inter-agency approach"* di keamanan nasional[115][116] – hal ini mendorong negara lain meniru model NSCS Singapura. Juga, para *alumni* intelijen Singapura (pensiunan pejabat) kerap diundang menjadi pembicara di konferensi internasional, menyuarakan perspektif Singapura (tanpa embel-embel resmi, tapi pengaruhnya ada). Sebagai contoh, Bilahari Kausikan (mantan pejabat MFA yang dekat dengan komunitas intel) aktif menulis soal bahaya pengaruh Tiongkok di Asia Tenggara, yang mempengaruhi opini publik regional dan memperkuat legitimasi kebijakan anti-intervensi Singapura[117][118].

Secara keseluruhan, aktivitas intelijen Singapura di Asia Tenggara telah menjadikannya pemain kunci dalam keamanan kawasan, meski ukurannya kecil. Negara-negara tetangga, termasuk Indonesia, umumnya menyambut kolaborasi kontra-teror dan maritim karena membantu kepentingan bersama. Namun ada kalanya kecemburuan muncul, menganggap Singapura "mata-telinga" Barat di ASEAN. Singapura berusaha mengimbanginya dengan transparansi terbatas – misal, mengajak perwira Indonesia memimpin CTIF, atau membuka data IFC untuk kepentingan bersama. Pola Singapura adalah "cooperative security": berbagi intel untuk keamanan kolektif sambil mengukuhkan posisinya sendiri. Dengan tantangan baru (seperti kehadiran pemain besar Tiongkok di kawasan), intelijen Singapura kemungkinan akan terus memainkan peran wasit netral yang memperingatkan negara ASEAN akan risiko, sekaligus menjaga agar Singapura tidak tersudut dalam rivalitas kekuatan besar.

Evaluasi Risiko dan Kelemahan Model Intelijen Singapura

Sekuat apapun, model intelijen Singapura bukannya tanpa celah. Dalam perspektif kontra-intelijen regional, beberapa risiko dan kelemahan dapat diidentifikasi:

- Infiltrasi dan Spionase Asing: Sebagai negara multietnis terbuka, Singapura bisa menjadi target empuk bagi intelijen asing, terutama Tiongkok dan Barat, untuk merekrut agen atau mempengaruhi kebijakan. Kasus Huang Jing (2017) menunjukkan adanya *agent of influence* asing yang beroperasi di Singapura[110]. Huang, akademisi terkemuka di LKY School, dituduh berkolaborasi dengan intel asing menyuplai "informasi istimewa" untuk mempengaruhi pejabat Singapura[119][112]. Ini indikasi bahwa intelijen asing melihat Singapura sebagai tempat strategis menanam pengaruh. Begitu pula skandal Dickson Yeo (2020): seorang PhD Singapura direkrut intel Tiongkok untuk mengumpulkan informasi di AS[120][121]. Yeo *pleaded guilty* di pengadilan AS atas menjadi agen ilegal Tiongkok[120]. Intel Singapura diketahui telah memantau kasus ini (MHA menyatakan "sudah mengetahui kasus Yeo sejak penangkapannya" oleh FBI)[122], namun faktanya Yeo bisa beroperasi beberapa tahun sebelum tertangkap di luar negeri. Reuters menyebut kasus Yeo *"menghidupkan kembali kekhawatiran bahwa Tiongkok merekrut aset*

intelijen di negara pulau yang dipercaya Barat namun tetap akur dengan Beijing"[123][118]. Artinya, profil Singapura yang bersahabat dengan semua pihak justru berisiko dimanfaatkan kedua belah pihak. Kelemahan ini: Singapura harus ekstra waspada terhadap warga atau penduduknya sendiri yang bisa ditarget intel asing – padahal mobilitas warga Singapura tinggi dan paspornya "emas" (bebas visa banyak negara), membuat mereka menarik bagi perekrut seperti Tiongkok[118]. Ini tantangan kontra-intelijen internal bagi ISD: mengawasi potensi "pelarian informasi" tanpa membuat iklim ketidakpercayaan di masyarakat.

- Trust Issues dengan Negara Tetangga: Meskipun Singapura banyak membantu keamanan regional, sebagian negara ASEAN masih menyisakan skeptisisme. Laporan akademis tentang *Our Eyes* mencatat resistensi birokrasi di Indonesia & Filipina menghambat pertukaran intelijen [48][124]. Faktor seperti kebocoran informasi dan budaya patron-klien membuat agensi enggan berbagi data sensitif[125]. Bagi Singapura, ini kelemahan eksternal: sebaik apapun intel Singapura, jika mitra tak mau berbagi balik, gambaran ancaman bisa timpang. Selain itu, kenangan persaingan lama (Singapura pernah dicurigai Malaysia menyadap komunikasi diplomatiknya di masa lalu) bisa mengekang kerjasama penuh. Singapura telah mencoba mengatasinya lewat transparansi terbatas (contoh: IFC bersifat open platform, AOE diusahakan *terintegrasi*), namun risiko tetap ada bahwa inisiatif integrasi intel akan terhambat oleh perbedaan politik domestik negara ASEAN.
- Ketergantungan pada Teknologi Asing: Demi teknologi maju, Singapura banyak bermitra dengan pihak luar (AS, Israel, Eropa). Ini menimbulkan ketergantungan strategis. Misal, penggunaan perangkat lunak asing untuk analitik berisiko ditanami *backdoor*. Hubungan erat dengan intel Barat juga punya harga: Singapura bisa terseret pertikaian adikuasa. Jika hubungan AS-Tiongkok memburuk, Singapura akan ditekan kedua pihak. Sudah muncul gejala: 2020 ketika AS-China saling tuduh spionase (penutupan konsulat), kasus Yeo memicu kekhawatiran bahwa Singapura jadi *proxy war* intel AS-China[126]. Dalam situasi ekstrem, Tiongkok bisa memandang Singapura terlalu mesra dengan AS (misal ikut menyadap kabel telekomunikasi untuk NSA[127]), lalu meningkatkan operasi intel di Singapura sebagai balasan. Ini perang bayangan yang riskan bagi Singapura.
- Kelemahan Sumber Daya Manusia: Meski program rekrutmen maju, Singapura tetap memiliki basis SDM terbatas. Intelijen adalah pekerjaan menantang dan menuntut komitmen tinggi. Ada kekhawatiran *burnout* atau kehilangan talenta ke sektor swasta (gaji di intel pemerintah mungkin kalah saing dibanding industri teknologi). SID mengakui perlu waktu lama merekrut karena proses penyaringan keamanan ketat (3-6 bulan)[128]. Ini dapat memperlambat regenerasi. Juga, sifat tertutup intelijen membuat sulit mendiversifikasi SDM – kendati diupayakan, mungkin minoritas tertentu masih kurang terwakili. Apalagi Singapura masyarakat majmuk: memastikan perwira intel dari berbagai etnis sama-sama loyal dan dipercaya merupakan tantangan historis (dulu Special Branch didominasi satu ras). Walau generasi muda lebih inklusif, intel tetap bidang sensitif. Selain itu, National Service yang jadi keunggulan, bisa pula jadi kelemahan bila tak dikelola baik: pelatihan NS yang singkat (2 tahun) mungkin tidak cukup menghasilkan ahli mendalam kecuali di program spesialis. Mereka bisa jadi "jack of all trades, master of none" jika kurikulumnya tak fokus.
- Risiko "Insider Threat" dan Keamanan Informasi: Seperti semua dinas intel, ancaman datang dari dalam berupa pembocoran rahasia atau pembelotan. Singapura nyaris tak pernah diterpa skandal bocor seperti WikiLeaks, namun bukan mustahil. Sistem penghargaan tertutup (petugas SID tak dapat medali publik, hanya medali rahasia setara *National Day Awards*[129]) bisa menimbulkan demotivasi bagi sebagian orang, atau justru frustrasi sehingga rentan dipengaruhi aktor luar. Intel

Singapura pun beroperasi dalam masyarakat sangat digital – potensi peretasan jaringan intel oleh musuh selalu ada. Pernah pada 2014, data pribadi 1.5 juta pasien SingHealth (termasuk PM Lee) dicuri hacker diduga negara asing. Walau bukan data intelijen, insiden ini lampu kuning bahwa bahkan sistem TI Singapura bisa ditembus. Jika sistem intel (misal database ISD) diretas asing, dampaknya akan parah. Keamanan siber internal karenanya sangat krusial; DIS Cyber Staff harus terus satu langkah di depan upaya penetrasi musuh.

- Kurangnya Oversight Independen: Dari sudut pandang *good governance*, model intelijen Singapura kurang mekanisme pengawasan legislatif atau yudisial. Keputusan intel banyak diambil tertutup oleh eksekutif. Ini efisien, tapi ada risiko kesalahan intel atau penyalahgunaan kekuasaan sulit dikoreksi. Penahanan tanpa pengadilan via ISA misalnya, bergantung sepenuhnya pada asumsi intel ISD. Dalam konteks regional, hal ini bisa disorot negara lain untuk mendiskreditkan Singapura (misal menuduh intel Singapura sewenang-wenang terhadap aktivis). Walau sejauh ini belum berdampak signifikan, di era media sosial, narasi tersebut bisa dihembuskan kompetitor untuk mengurangi *moral authority* Singapura dalam menyerukan supremasi hukum.
- Kelemahan Cakupan HUMINT Eksternal: SID yang sangat rahasia dan dengan personel terbatas mungkin kesulitan menyaingi jangkauan HUMINT negara besar di wilayah. Contoh, untuk mengintai kelompok militan di Mindanao atau Kalimantan, intel Singapura perlu berkolaborasi atau mengirim petugas yang “terlihat seperti lokal”. Sebagai negara minoritas Melayu, mengirim etnis Tionghoa Singapura ke lapangan misalnya bisa kurang efektif karena mencolok. Meskipun Singapura punya komunitas Melayu/India, jumlah agen yang bersedia operasi lama di lapangan luar negeri mungkin tidak banyak. Ini potensi kelemahan jika terlalu bergantung pada intel teknis. *However*, Singapura sebagian mengatasi ini dengan informal diplomacy – menggunakan jalur kerjasama resmi agar tak perlu pasang HUMINT resiko tinggi. Tetapi di kasus seperti penyusupan ISIS ke Marawi 2017, mungkin intel Singapura agak tertinggal karena tidak punya *ground assets* langsung di sana dan harus mengandalkan info Filipina/AS.

Melihat semua itu, Singapura berupaya memitigasi kelemahan melalui kebijakan adaptif: memperketat screening (mencegah insider threat), hukum FICA (mencegah pengaruh asing), diversifikasi rekrutmen (menutup celah kurang HUMINT), dan kerjasama luas (menambal keterbatasan jangkauan). Namun, dari perspektif kontra-intelijen regional, negara tetangga dan kekuatan besar pasti terus menguji sistem Singapura. Keberhasilan Singapura menjaga *fine balance* antara keterbukaan ekonomi dan keamanan nasional akan ditentukan oleh kemampuan intelijennya menghadang ancaman tersembunyi tanpa mengisolasi diri.

Kesimpulan: Selama satu dekade terakhir, intelijen Singapura telah berkembang menjadi salah satu yang paling terorganisir, canggih, dan terpadu di Asia. Struktur tiga serangkai (ISD-SID-DIS) dalam koordinasi PMO memastikan liputan ancaman 360 derajat – dari ancaman teroris lokal hingga rivalitas kekuatan besar global*[19][20]*. Didukung think tank berpengaruh, aliansi strategis dengan negara maju, serta dorongan inovasi teknologi (SIGINT, siber, AI), Singapura mampu men punch di atas bobotnya dalam hal intelijen dan keamanan. Peranannya di Asia Tenggara sebagai motor integrasi intelijen telah meningkatkan keamanan kolektif kawasan, sekaligus mengamankan kepentingan nasionalnya. Meski begitu, intelijen Singapura harus terus beradaptasi menghadapi risiko infiltrasi asing dan dinamika geopolitik yang berubah cepat. Model tertutup namun tangkas yang mereka terapkan tampaknya sejauh ini berhasil – intelijen Singapura jarang terekspos gagal publik, malah kerap diakui membantu mencegah krisis. Bagi Indonesia dan negara tetangga, intelijen Singapura ibarat dua sisi mata uang: *mitra taktis terpercaya*, tapi juga *aktor waspada* yang kemampuan dan agenda strategisnya perlu terus dipahami. Dengan lanskap ancaman 2025 ke depan mencakup *cyberwarfare*, *grey-zone operations*,

dan terorisme yang bertransformasi, kecerdikan dan kewaspadaan intelijen Singapura akan kembali diuji. Namun melihat rekam jejak satu dasawarsa ini, Singapura menunjukkan kapasitas menyeimbangkan keamanan dan kepentingan strategisnya secara lincah dan tegas, menjadikannya model unik intelijen negara kecil di pentas global.

Referensi:

- Internal Security Dept (ISD) vs Security & Intelligence Division (SID) – fokus tugas[21].
- SID bekerja erat dengan agensi pemerintah lain dan mitra internasional dalam hadapi terorisme, siber, dsb[20].
- SID melapor ke PMO meski di bawah MINDEF, otonom dan rahasia, direktur setara Perm. Sec[4] .
- NSCS dibentuk 2004 di PMO, memaksa SID-ISD berbagi info yang sebelumnya terpisah[19].
- Think tank CENS (RSIS) sebagai unit riset kebijakan keamanan nasional yang relevan kebijakan [26].
- Kolaborasi intelijen Singapura-Australia: dugaan penyadapan kabel bawah laut bersama ASD[43].
- Kemitraan Singapura-AS dalam AI dan data analytics untuk perkuat interoperabilitas[36].
- Kemitraan Singapura-UK ditingkatkan mencakup intelijen dalam *Strategic Partnership 2023*[39].
- Pendirian *Digital and Intelligence Service (DIS)* 2022 mengintegrasikan C4I dan siber SAF[8][130] .
- DIS dilengkapi Joint Intelligence Command (Counter-Terrorism Intel Group, dsb) untuk *early warning* operasi SAF[11].
- DIS membentuk Digital Ops-Tech Centre guna kembangkan inti digital melek data science & AI [14].
- SID meluncurkan situs web 2021, buka rekrutmen umum demi jaring talenta beragam dan jelaskan misi agensi[131][73].
- SID dulu rekrut lulusan via “tea session”, kini juga bidik profesional mid-career: ekonom, pengacara, banker, dll[76][75].
- Perekrutan lebih terbuka untuk hindari *groupthink* – perlu perspektif berbeda & tantang pemikiran mapan[79][81].
- Michael (SID) memaparkan misi SID berevolusi: dari fokus regional 1960-an, ke terorisme pasca-2001, hingga kini ancaman kompleks (siber, perang informasi, pandemi, perubahan iklim)[132] [133].
- Sophie (analis SID) kisahkan direkrut lewat *tea session*, tertarik karena minat internasional – di SID ia berkesempatan belajar bahasa asing & teknologi analisis data[32][82].
- Sophie jelaskan kerahasiaan: ia bilang ke orang bahwa ia kerja di MINDEF dengan pekerjaan “sensitif”, dan keluarga mengerti[101].
- Michael ungkap peran SID dalam operasi multi-lembaga mengejar teroris JI awal 2000-an yang kabur ke luar – sukses dengan beri peringatan dini ke mitra/regional[102][104].
- Michael sebut SID bantu pembentukan Joint Counter Terrorism Centre (JCTC) 2004 yang kemudian diintegrasi ke NSCS sebagai National Security Research Centre[18].
- SID dukung gagalkan rencana serangan teroris ke Marina Bay Sands tahun 2016[105].
- Menhan Ng Eng Hen resmikan CTIF, fasilitas multilateral intelijen kontra-teror di Singapura – berbagi intel dan peringatan dini ancaman regional[49][51].
- CTIF disebut penting sinergikan upaya kontra-teror dengan intel kolektif dan metode berbasis data, operasi banyak rahasia demi keamanan regional[51].

- Dr Ng puji CTIF sukses deteksi penyebaran ideologi ekstrem di region sehingga diikuti aksi aparat regional[66].
- CTIF operasional sejak Jan 2021, telah hasilkan intel tepat waktu dengan negara mitra dan bantu upaya kolektif lawan teror[50].
- IFC (Maritime Security centre) didirikan RSN 2009, posisinya di Changi C2 Centre, untuk info-sharing ancaman maritim (perompakan, teror maritim, penyelundupan, dsb)[134][135].
- 24 negara kirim 155 International Liaison Officers (ILO) ke IFC sejak berdiri (saat ini 19 ILO dari 18 negara di sana, plus 12 personel RSN)[53][106].
- IFC punya 97 link dari 41 negara, salah satu dari 4 *Technical Leading Navies* di jaringan *Trans-Regional Maritime Network* global[107][136].
- IFC membantu bentuk kebiasaan saling tukar info di region, melalui portal multilateral ASEAN ISP, WPNS, Malacca Straits Patrol, dsb[137][138].
- IFC juga libatkan komunitas pelayaran (VCR system, Shared Awareness Meetings) dan telah membantu operasi pencarian MH370 melalui jejaring kapal[139][140].
- Capaian IFC: kolaborasi kuat lintas negara hasilkan penurunan 62% insiden perompakan 2015 ke 2018 (200 turun ke 76 kasus). Di Selat Malaka/Singapura turun 92% (104 ke 8 kasus) periode sama[54][55].
- Contoh kontribusi IFC: tracking kapal Sunrise Glory dicurigai 3 bulan, info via ILO Indonesia bantu TNI AL tangkap kapal tsb bawa 1 ton sabu (Feb 2018)[56][57].
- Contoh lain: Mei 2016 kapal tanker Hai Soon 12 hilang kontak, IFC pakai tracker GPS sekunder milik pemilik kargo untuk temukan lokasinya, info ke ILO, TNI AL bergerak dan temukan kapal dibajak 9 perompak (mau curi muatan), semua ABK selamat[109][141].
- Huang Jing diidentifikasi MHA sebagai “agent of influence” asing, berusaha pengaruhi pejabat Singapura dengan info “privileged” dan bekerja sama dengan agen intel asing – dinilai subversif, intervensi asing[110][119].
- MHA tak sebut negara mana, banyak anggap China (kelahiran Huang). PR Huang dan istri dicabut, mereka dideportasi 2017. Huang disebut gunakan posisinya untuk majukan agenda negara asing dengan cara terselubung[111][142].
- Huang diketahui berinteraksi dan bekerja sama dengan organisasi intel asing untuk pengaruhi kebijakan luar negeri Singapura dan opini publik[112].
- Dickson Yeo (Jun Wei Yeo), warga SG 39 tahun, mengaku bersalah di pengadilan AS Juli 2020 atas agen ilegal intel China[123][120]. Ia direkrut ketika hadir forum di Beijing 2015, sempat fokus target Asia Tenggara lalu alihkan ke AS 2019, menggunakan konsultan palsu & LinkedIn untuk jaring orang dengan akses informasi rahasia[121][143].
- Yeo membayar target (termasuk seorang sipil AS akses program jet tempur) agar tulis laporan baginya[144][145].
- Yeo ternyata mantan mahasiswa bimbingan Huang Jing di NUS – Huang (yang diusir SG) kaget dan senang Yeo tertangkap, menyebut Yeo “ingin dianggap hebat, punya rasa insecure”[146][147].
- Kemenhan SG (MINDEF) meluncurkan Cyber NSF Scheme 2018 untuk ambil bakat siber di pool NS, latih operasional pertahanan siber[90][148].
- Cyber NSF Scheme bekerja sama SIT (2018) dan kemudian NUS (2020) untuk Work-Learn Programme 3-4 tahun; NSFs dapat training akademik paruh waktu selaras on-job training, dapat kredit kuliah yang bisa dihitung ke gelar S1 Infosec[92][93].
- WLP SIT & NUS rancang kurikulum komprehensif imbangi tugas operasional; NSFs bisa lulus sarjana bersamaan dengan rekan seangkatan meski NS mereka lebih lama[149][150].

- Respon ke Cyber Specialist Award bagus, ~170 NSF sudah menerima award ini (4 angkatan), angkatan perdana lulus Agustus 2019*[95][96]*.
- Lulusan kursus kadet spesialis siber ditempatkan di berbagai peran operasional pertahanan siber (incident response, digital forensics, malware analysis, pentest) untuk lindungi jaringan MINDEF/SAF*[97][151]*.
- Setelah penugasan, mereka lanjut kuliah paruh waktu. Pelamar harus punya pengetahuan dasar siber, melalui rangkaian tes ketat (kripto, arsitektur sekuriti, dll)*[91][152]*.
- Cyber NSF Scheme bersama dengan skema ahli C4 (C4X) berbaju seragam dan Defence Cyber Expert (DCX) sipil, membentuk tenaga kerja siber ahli pertahanan*[99][153]*. Program ini sekaligus berkontribusi ke ekosistem siber nasional dengan kembangkan talenta sejak muda*[153][154]*.

[1] [18] [21] [32] [35] [65] [71] [72] [73] [74] [75] [76] [77] [78] [79] [80] [81] [82] [83] [101] [102] [103] [104] [105] [128] [131] [132] [133] Singapore intelligence officers open up as SID seeks to recruit more diverse talent – CNA

https://www.channelnewsasia.com/singapore/sid-singapore-intelligence-officers-security-recruitment-2049961

[2] Singapore – United States Department of State

https://www.state.gov/reports/country-reports-on-terrorism-2021/singapore

[3] [4] [5] [6] [7] [16] [19] [24] [38] [43] [88] [127] [129] Security and Intelligence Division – Wikipedia

https://en.wikipedia.org/wiki/Security_and_Intelligence_Division

[8] [9] [10] [11] [12] [13] [14] [15] [63] [89] [100] [130] Fact Sheet: The Digital and Intelligence Service | Ministry of Defence

https://www.mindef.gov.sg/news-and-events/latest-releases/28oct22_fs

[17] [22] [23] [115] [116] CO04036 | Assessing the Structure of the New National Security Strategy – RSIS

https://rsis.edu.sg/rsis-publication/rsis/632-assessing-the-structure-of-the/

[20] Our Mission

https://www.sid.gov.sg/about-us/our-mission/

[25] ISEAS – Yusof Ishak Institute – Wikipedia

https://en.wikipedia.org/wiki/ISEAS_%E2%80%93_Yusof_Ishak_Institute

[26] Useful Links

https://www.nscs.gov.sg/useful-links/

[27] Centre of Excellence for National Security CENS – RSIS

https://rsis.edu.sg/research/cens/

[28] ISEAS – Yusof Ishak Institute (ISEAS) – Security & Sustainability

https://securesustain.org/abstract/iseas-yusof-ishak-institute-iseas/

[29] [30] [42] [48] [124] [125] "Bureaucratic Resistance and The Challenge of Implementing ASEAN Our Eyes" by Chaula Rininta Anindya

https://scholarhub.ui.ac.id/global/vol24/iss2/1/

[31] [114] Singapore: Foreign Interference (Countermeasures) Act

https://oneasia.legal/en/4163

[33] [60] [61] [62] [64] [69] [70] Singapore's defence sector sees more coordinated efforts in AI and cybersecurity

https://govinsider.asia/intl-en/article/singapores-defence-sector-sees-more-coordinated-efforts-in-ai-and-cybersecurity

[34] About Singapore-US Relations

https://www.mfa.gov.sg/Overseas-Mission/Washington/About-Singapore-US-Relations

[36] [37] [58] [59] [68] U.S., Singapore Cooperate on Data Analytics, Artificial Intelligence > U.S. Department of Defense > Defense Department News

https://www.defense.gov/News/News-Stories/Article/Article/3839335/us-singapore-cooperate-on-data-analytics-artificial-intelligence/

[39] [40] Ministry of Foreign Affairs Singapore – 20230909 UK-SG Strategic Partnership

https://www.mfa.gov.sg/Newsroom/Press-Statements-Transcripts-and-Photos/2023/09/20230909-UK-SG-Strategic-Partnership

[41] UK agrees new strategic partnership with Singapore – GOV.UK

https://www.gov.uk/government/news/uk-agrees-new-strategic-partnership-with-singapore

[44] [45] SINGAPORE/ISRAEL : Singapore turns to Israeli cyber spies again – 03/04/2019 – Intelligence Online

https://www.intelligenceonline.com/international-dealmaking/2019/04/03/singapore-turns-to-israeli-cyber-spies-again,108351899-art

[46] National Cybersecurity Partnership: Singapore and Israel | SGInnovate

https://www.sginnovate.com/event/national-cybersecurity-partnership-singapore-and-israel

[47] “The most strategic country in the world”: Singapore is doubling …

https://www.calcalistech.com/ctechnews/article/b1l7y50bkg

[49] [50] [51] [66] Dr Ng: CTIF Supports Regional Security Agencies in the Collective Fight against Terrorism | Ministry of Defence

https://www.mindef.gov.sg/news-and-events/latest-releases/21sep22_nr

[52] Embassy of the Philippines in Singapore

https://www.philippine-embassy.org.sg/philippines-assumes-leadership-of-counter-terrorism-information-facility-in-singapore/

[53] [54] [55] [56] [57] [106] [107] [108] [109] [134] [135] [136] [137] [138] [139] [140] [141] Fact Sheet on Information Fusion Centre (IFC) and Launch of IFC Real-Time Information-Sharing System (IRIS) | Ministry of Defence

https://www.mindef.gov.sg/news-and-events/latest-releases/14may19_fs

[67] AI, Machine Learning & Big Data Laws 2025 | Singapore

https://www.globallegalinsights.com/practice-areas/ai-machine-learning-and-big-data-laws-and-regulations/singapore/

[84] [86] [87] Security and Intelligence Division

https://www.sid.gov.sg/

[85] Internship & Scholarships

https://www.sid.gov.sg/careers-with-us/internship-scholarships/

[90] [91] [92] [93] [94] [95] [96] [97] [99] [148] [149] [150] [151] [152] [153] [154] Fact Sheet: Update on the Cyber Specialist Award | Ministry of Defence

https://www.mindef.gov.sg/news-and-events/latest-releases/29may20_fs

[98] PIONEER COHORT OF NSF CYBER SPECIALISTS GRADUATE

https://www.defencepioneer.sg/pioneer-articles/PIONEER-COHORT-OF-NSF-CYBER-SPECIALISTS-GRADUATE

[110] [111] [112] [113] [119] [142] Huang Jing, Chinese-American academic expelled by Singapore, is working in Beijing and has ‘no hard feelings’ – TODAY

https://www.todayonline.com/world/huang-jing-chinese-american-academic-expelled-singapore-working-beijing-and-has-no-hard

[117] [118] [120] [121] [122] [123] [126] [143] [144] [145] [146] [147] Singapore spy case reawakens fears China recruiting on island state | Reuters

https://www.reuters.com/article/world/singapore-spy-case-reawakens-fears-china-recruiting-on-island-state-idUSKCN24T0ZU/

Daftar Pustaka

- CNA. (2021, July 19). *Singapore's external intelligence agency launches website to recruit more officers*. CNA. https://www.channelnewsasia.com/singapore/sid-external-intelligence-agency-website-recruitment-2014216

- CNA. (2021, July 19). *Singapore's external intelligence agency SID goes public, launches recruitment website*. The Straits Times. https://www.straitstimes.com/singapore/sid-goes-public-for-first-time

- CNA. (2022, September 27). *New SAF Digital and Intelligence Service inaugurated to deal with threats in digital domain*. CNA. https://www.channelnewsasia.com/singapore/saf-digital-and-intelligence-service-inaugurated-threats-digital-domain-2964701

- CNA. (2022, September 28). *CT Information Facility officially inaugurated in Singapore*. CNA. https://www.channelnewsasia.com/singapore/counter-terrorism-information-facility-ctif-singapore-ng-eng-hen-2964831

- CNA. (2020, July 25). *Singaporean pleads guilty in US to working for Chinese intelligence*. CNA. https://www.channelnewsasia.com/world/singapore-dickson-yeo-guilty-chinese-intelligence-651026

- CNA. (2017, August 4). *Academic Huang Jing permanently banned from Singapore for being agent of influence*. CNA. https://www.channelnewsasia.com/singapore/academic-huang-jing-banned-agent-influence-907221

- Defence Science and Technology Agency (DSTA). (2024, March 20). *DSTA and MINDEF explore responsible use of AI in defence*. MINDEF Singapore. https://www.mindef.gov.sg/web/portal/mindef

- ISEAS–Yusof Ishak Institute. (n.d.). *About ISEAS*. https://www.iseas.edu.sg

- Ministry of Defence Singapore. (2024, July 18). *Singapore and US sign Statement of Intent to strengthen cooperation in data analytics and AI*. MINDEF Singapore. https://www.mindef.gov.sg/web/portal/mindef/news-and-events

- Ministry of Defence Singapore. (2022, September 28). *Speech by Minister for Defence Dr Ng Eng Hen at the inauguration of the SAF Digital and Intelligence Service*. MINDEF Singapore. https://www.mindef.gov.sg/web/portal/mindef/news-and-events

- Rajaratnam School of International Studies (RSIS). (n.d.). *Centre of Excellence for National Security (CENS)*. https://www.rsis.edu.sg/research/cens/

- Reuters. (2020, July 25). *Singaporean pleads guilty in US to working for Chinese intelligence*. Reuters. https://www.reuters.com/article/singapore-intelligence-china-idUSKCN24Q0Q3

- Straits Times. (2023, September 14). *Singapore and Britain agree to deepen cooperation in defence, intelligence, cybersecurity*. The Straits Times. https://www.straitstimes.com/singapore/singapore-uk-to-deepen-defence-intelligence-cybersecurity-cooperation

- Today Online. (2018, February 15). *How Singapore's Information Fusion Centre helps tackle piracy and terrorism at sea*. Today. https://www.todayonline.com/singapore/how-singapores-information-fusion-centre-helps-tackle-piracy-and-terrorism-sea-895931

- Today Online. (2018, June 28). *MINDEF launches Cyber NSF Scheme to train young national servicemen in cyber defence*. Today. https://www.todayonline.com/singapore/mindef-launches-cyber-nsf-scheme-educate-young-ns-men-cyber-defence